National Infrastructure Protection Center
CyberNotes

Issue #2000-25 66F-HQ-A1276002 Sub B 2.4 December 18, 2000

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between December 14, and November 27, 2000. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Alex Heiphetz Group, Inc.[1] Windows NT 4.0, Unix	EZShopper 2.0, 3.0	A vulnerability exists in loadpage.cgi which could let a remote malicious user gain sensitive information.	No workaround or patch available at time of publishing.	EZShopper Directory Disclosure CVE Name CAN-2000-1092	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[1] NSFOCUS Security Advisory, SA2000-09, December 13, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire[2]	ColdFusion Server 4.5.1	A vulnerabilty exists if the search engine is enabled upon installation, which could let remote malicious user cause a Denial of Service.	Workaround taken from an Allaire Security Best Practice Bulletin: You should remove the CFDOCS directory. In a typical installation, that directory resides at: {webroot}/CFDOCS/	ColdFusion Sample Script Denial of Service	Low	Bug discussed in newsgroups and websites.
Alt-N Technologies[3] Windows 95/98/NT 4.0/2000	MDaemon 3.5.1	A vulnerability exists in the "lock" feature which could let a malicious user gain entry to the interface with administrative privileges.	No workaround or patch available at time of publishing.	MDaemon 'Lock Server' Bypass	**High**	Bug discussed in newsgroups and websites.
Apache Group[4] Windows NT 4.0/2000	Apache 1.3	A security vulnerability exists in systems that have Apache and PHP installed, which could allow a remote malicious user to access files outside the document root directory.	No workaround or patch available at time of publishing.	Apache Web Server with Php File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
BroadVision[5]	One-To-One Enterprise 1.0	A security vulnerability exists when a malicious user requests a non-existent file. This will reveal the physical path of server files.	No workaround or patch available at time of publishing.	One-To-One Enterprise Path Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
CatSoft[6] Windows 3.1/95/98/NT 4.0/2000	Serv-U 2.4, 2.5	A security vulnerability exists which could allow a remote malicious user to gain access to files and directories outside the normal scope of the user's FTP home directory. The vulnerability can be used to completely compromise the operating system.	Upgrade to Serv-U FTP 2.5i. available at: http://ftpserv-u.deerfield.com/download/getftpservu.cfm	Serv-U FTP Directory Traversal	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
CGI Script Center[7] Windows NT 4.0/2000, Unix	Subscribe Me Lite 2.0	A vulnerability exists in the administration script that could let a malicious user obtain access to the script's administration panel and delete arbitrary members from the mailing lists supported by the vulnerable script.	No workaround or patch available at time of publishing.	Subscribe-Me Lite Administration Access	Medium	Bug discussed in newsgroups and websites.

[2] Bugtraq, December 8, 2000.
[3] Bugtraq, December 13, 2000.
[4] CHINANSL Security Advisory, CSA-200011, December 6, 2000.
[5] Securiteam, December 10, 2000.
[6] Securax-SA-09 Security Advisory, December 5, 2000.
[7] Bugtraq, December 12, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Cisco[8]	Catalyst 4000 and 5000 images running version 4.5(2) up to 5.5(4) and 5.5(4a); Catalyst 6000 images running version 5.3(1)CSX, up to and including 5.5(4), 5.5(4a)	The telnet server that is built into the Catalyst firmware for remote administration contains a memory leak vulnerability that can result in a Denial of Service.	Workaround and patch information available at: http://www.cisco.com/warp/public/707/catalyst-memleak-pub.shtml.	Cisco Catalyst Memory Leak Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Endymion[9] Windows, Unix	MailMan WebMail 3.0.25 and prior	A vulnerability exists due to insecure handling of a call to the Perl open() function which could let a remote malicious user run arbitrary commands with web server privileges.	Upgrade available at: http://www.endymion.com/products/mailman/download.htm	MailMan WebMail Remote Arbitrary Command Execution	High	Bug discussed in newsgroups and websites.
Great Circle Associates[10]	Majordomo 1.94.4, 1.94.5	A vulnerability exists in the authentication system that could allow a remote malicious user to execute administrative commands.	No workaround or patch available at time of publishing.	Majordomo Config-file admin_password Configuration	High	Bug discussed in newsgroups and websites.
IBM[11] Windows NT 4.0/2000	DB2 Universal Database for Windows NT 6.1, 7.1	A vulnerability exists in the way certain queries are handled which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	DB2 Universal Database for Windows NT SQL Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[12] Unix	AIX 4.{3,2}.x	Several buffer overflow vulnerabilities exist in the setuid and setgid binaries (libs) which could allow a local malicious user to gain root access. A vulnerability in 'portmir' can also be used to kill other processes as root.	Upgrades available at: http://techsupport.services.ibm.com/rs6k/fixes.html	AIX Multiple Buffer Overflow Vulnerabilities	High	Bug discussed in newsgroups and websites.

[8] Cisco Advisory, CI-00.11, December 6, 2000.
[9] Secure Reality Pty Ltd. Security Advisory , SRADV00005, December 6, 2000.
[10] Bugtraq, December 1, 2000.
[11] Securiteam, December 14, 2000.
[12] Securiteam, December 4, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
IBM[13] Windows NT 4.0/2000, Unix	DB2 Universal Database for Linux 6.1; DB2 Universal Database for Windows NT 6.1	A vulnerability exists which could allow a malicious user to log in as administrator.	Recommended Fix: Change the default username and password.	DB2 Universal Database Known Default Password	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Inktomi (formerly known as Infoseek)[14] Windows NT 4,0, Unix	Ultraseek Server 3.0	Two security vulnerabilities exist which could allow a malicious user to get the absolute path and source code of Ultraseek Server add-ons.	No workaround or patch available at time of publishing.	Ultraseek Information and Source Disclosure Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Ipswitch[15] Windows NT 4.0/2000	IMail 6.0.5	A Denial of Service vulnerability exists when a base 64encoded SMTP AUTH password containing 80 to 136 bytes is entered.	No workaround or patch available at time of publishing.	IMail Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Keware Technologies[16] Windows 95/98/NT 4.0/2000	HomeSeer 1.4	A directory traversal vulnerability exists which could let a remote malicious user gain access to any known file outside of the HomeSeer directory on the root directory. This could lead to a complete compromise of the host.	This has been fixed in the 1.4.29 (beta-) version which is available at: http://www.keware.com/kewarebeta.htm	HomeSeer Directory Traversal	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
KTH (Royal Institute of Technology, Sweden)[17] Unix	Kerberos 4 1.0.3-1.0 and prior	Multiple vulnerabilities exist which could lead to local and remote root compromise if the system supports Kerberos authentication and uses the KTH implementation.	OpenBSD has a patch available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/2.8/common/006_kerberos.patch	Multiple Kerberos Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
Leif M. Wright[18]	simplestmail.cgi 1.0	A vulnerability exists due to insecurely structured calls to the open() function, which could let a malicious user, execute arbitrary shell commands.	No workaround or patch available at time of publishing.	simplestmail.cgi Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[13] eSecurityOnline.com Free Vulnerability Alert 3225, December 14, 2000.
[14] Securiteam, December 13, 2000.
[15] Bugtraq, December 7, 2000.
[16] Strumpf Noir Society Advisories, December 7, 2000.
[17] Bugtraq, December 8, 2000.
[18] Bugtraq, December 11, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Leif M. Wright[19]	Everything form.cgi 2.0	An input validation vulnerability exists because the script fails to properly filter shell commands from user-supplied input which could let a malicious user run arbitrary shell commands.	No workaround or patch available at time of publishing.	everythingform.cgi Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Leif M. Wright[20]	simplestguest.cgi 2.0	A vulnerability exists due to an insecure call to the open() function which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Simplest-guest.cgi Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
MetaProducts[21]	Offline Explorer 1.0x, 1.1x, 1.2x, 1.3x	A vulnerability exists which could let a remote malicious user retrieve a directory listing and browse its contents without any authorization.	Upgrade available at: http://www.metaproducts.com/download/oesetup.exe	Offline Explorer File System Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[22] Windows 95/98/NT 4.0/2000	Internet Explorer 5.x	Three security vulnerabilities exist: the “Browser Print Template” vulnerabilty which could enable a malicious web site operator to take unauthorized actions on the computer of a user who visited their site; the "File Upload via Form" vulnerability, which could enable a malicious web site operator to read files on a visiting user's computer; and new variants of the "Scriptlet Rendering" and "Frame Domain Verification" vulnerabilities, both of which could enable a malicious web site operator to read files on a visiting user's computer.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-093.asp	Internet Explorer Browser Print Template, File Upload via Form, And Scriptlet Rendering and Frame Domain Verification Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[19] Bugtraq, December 11, 2000.
[20] Bugtraq, December 14, 2000.
[21] Bugtraq, December 7, 2000.
[22] Microsoft Security Bulletin, MS00-093, December 1, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[23] Windows NT 4.0/2000	Microsoft IIS Far East Edition 4.0, 5.0	A vulnerability exists when requests containing double-byte character sets (DBCS) are requested, which could let a malicious user get sensitive information contained within the web root. The editions that are affected include: Traditional Chinese, Simplified Chinese, Japanese, and Korean (Hangeul).	Unofficial workaround (NSFOCUS): 1) Remove unnecessary ISAPI mapping like HTR, HTW, IDQ, etc. 2) Turn on "Check that file exists" option in every necessary ISAPI mapping. 3) If you are using IIS 4.0 < SP6, update to SP6 **Note:** This vulnerability affects IIS prior to SP6. The problem was resolved with the release of SP6.	IIS Far East Edition DBCS File Disclosure CVE Name CAN-2000-1090	Medium	Bug discussed in newsgroups and websites.
Microsoft[24] Windows 95/98/NT 4.0/2000	Data Engine 1.0, 2000; SQL Server 7.0, 2000	Several buffer oveflow vulnerabilities exist which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-092.asp	Microsoft Extended Stored Procedure Parameter Parsing CVE names CAN-2000-1081 CAN-2000-1082 CAN-2000-1083 CAN-2000-1084 CAN-2000-1085 CAN-2000-1086 CAN-2000-1087 CAN-2000-1088	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Microsoft[25] Windows NT 4.0/2000	Windows NT 4.0 Server, Enterprise Edition, Windows 2000 Server, Advanced Server	A buffer overflow vulnerability exists in an optional service, which could allow a malicious user to execute arbitrary code on a remote server that is running the service.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-094.asp	Windows NT Phone Book Service Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[23] NSFOCUS Security Advisory, SA2000-08, December 13, 2000.
[24] Microsoft Security Bulletin, MS00-092, December 1, 2000.
[25] Microsoft Security Bulletin, MS00-094, December 5, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[26, 27] Windows NT 4.0/2000	Windows NT 4.0, 4.0 Server, Enterprise Edition, Terminal Server Edition; Windows 2000 Professional, 2000 Server, 2000 Advanced Server	A vulnerability exists in the default permissions of three keys: the SNMP Parameters key; the RAS (Remote Access Service) Administration key; and the MTS (Microsoft Transaction Server) Package Administration key which could allow a malicious user to gain additional privileges.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-095.asp	Windows NT Registry Permissions	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[28] Unix	Jason Hines phpWebLog 0.4.2	A vulnerability exists in common.inc.php which could allow a remote malicious user to bypass the administrative authentication protection and take administrative control of the message board.	The author is aware of the problem and a updated version will be available soon. Unofficial workaround (Securiteam): Change the default SiteKey.	phpWebLog Administrator Authentication Bypass	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[29] Unix	Joseph Engo phpGroupWare 0.9.6 and prior	A vulnerability exists in the include() function of php which could allow a remote malicious user to execute malicious code.	Upgrade available at: http://www.phpgroupware.org/downloads.php?filename=phpGroupWare-0.9.7.tar.gz	phpGroupWare Remote Include File	**High**	Bug discussed in newsgroups and websites
Multiple Vendors[30] Unix	Eric Rescorla ssldump 0.9b1 and previous	A vulnerability exists in the way ssldump handles format strings which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ssldump Format String	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[31] Unix	Colten Edwards BitchX 1.0c17	Two security vulnerabilities exist which could allow a remote malicious user to execute arbitrary code.	Upgrade to the latest package available: **RedHat:** ftp://updates.redhat.com/powertools/ **OpenLinux:** ftp://ftp.calderasystems.com/pub/updates/	BitchX Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[32] BeOS, Unix	Leif M. Wright ad.cgi 1.0	A vulnerability exists in the script which may allow a remote malicious user to gain access to restricted resources and execute arbitrary commands.	No workaround or patch available at time of publishing.	Leif M. Wright ad.cgi Unchecked Input	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[26] Microsoft Security Bulletin, MS00-095, December 6, 2000.
[27] Microsoft Security Bulletin, MS00-096, December 6, 2000.
[28] Securiteam, December 7, 2000.
[29] Secure Reality Pty Ltd. Security Advisory, SRADV00006, December 6, 2000.
[30] Bugtraq, December 8, 2000.
[31] eSecurityOnline.com Free Vulnerability Alert 3227, December 14, 2000.
[32] Bugtraq, December 11, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[33] Unix	Lexmark MarkVision 4.3 and previous	Several buffer overflow vulnerabilities exist which could let a malicious user gain elevated privileges and administrative access.	Upgrade available at: ftp://ftp.lexmark.com/pub/driver/unix/MarkVision/V4.4/	Lexmark MarkVision Printer Driver Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[34] Unix	APC Apcupsd 3.7.2	A vulnerability exists in the Unix daemon which could allow a malicious user to cause a Denial of Service.	Linux Mandrake has released updated Apcupsd packages available at: http://www.linux-mandrake.com/en/ftp.php3	APC Apcupsd Local Denial of Service	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[35] Unix	Linux kernel 2.2.10, 2.2.12-2.2.17	A vulnerability exists in the Linux implementation of ptrace which could allow a malicious user to gain sensitive information from non-readable not-setuid executable files.	No workaround or patch available at time of publishing.	Linux Non-Readable File Ptrace	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[36] Unix	Igor Khasilev Oops Proxy Server 1.4.22 and previous	Multiple buffer overflow vulnerabilities exist which could allow a malicious user to execute arbitrary code.	Upgrade to proxy 1.5.0.	Multiple Vendor Oops Proxy Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Nokia[37]	Nokia IP440 1.0	A buffer overflow vulnerability exists in the firewall implementation, which could allow a malicious user to execute arbitrary code.	This vulnerability will be fixed in the next scheduled release of IPSO (Nokia's OS). **Workaround:** 1. Do not allow Voyager access from untrusted networks (e.g., the Internet). 2. Use good generally accepted practice regarding password selection and confidentiality (as always). 3. Consider disabling monitor (read-only administrator) access. 4. Use the provided SSH with port redirection (IPSO 3.2.1 and earlier) or embedded SSL (IPSO 3.3 and later) to encrypt http traffic to Voyager to prevent an attacker from eavesdropping on the password.	Nokia IP440 Remote Denial of Service	**High** **(High if DDoS best practices not in place).**	Bug discussed in newsgroups and websites.
RedHat[38] Unix	Linux 6.0-6.2 sparc, i386, alpha	A race vulnerability exists which could let a malicious user corrupt arbitrary files on the system.	Patch available at: ftp://updates.redhat.com/powertools/6.2/noarch/diskcheck-3.1.1-10.6x.noarch.rpm	RedHat Linux diskcheck Race Condition	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[33] Secure Reality Pty Ltd. Security Advisory, SRADV00007, December 7, 2000.
[34] Bugtraq, December 6, 2000.
[35] Bugtraq, November 30, 2000.
[36] Packet Knights Advisory 001, December 11, 2000.
[37] Bugtraq, November 27, 2000.
[38] Red Hat Inc. Security Advisory, RHSA-2000:122-04, December 4, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Roaring Penguin Software[39] Unix	PPPoE 2.0-2.4	A vulnerability exists in the way TCP packets are handled when the Clamp_MSS option is used, which could let a remote malicious user cause a Denial of Service.	Upgrade to rp-pppoe 2.5 available at: http://www.roaringpenguin.com/pppoe/	Roaring Penguin PPPoE Denial of Service	Low	Bug discussed in newsgroups and websites.
SmartStuff[40] Windows 95/98/ME	FoolProof Security 3.9	A vulnerability exists which could let a malicious user circumvent the security measures and even remove it entirely from the system.	No workaround or patch available at time of publishing.	FoolProof Security Program Restriction Bypass	Medium	Bug discussed in newsgroups and websites.

Sun Microsystems, Inc.[41]
Windows 98/98/NT, Unix
	Sun Java HotSpot Performance Engine 1.0, 1.0.1;
	Sun JDK (Linux Production Release) 1.2.2_05, 1.2.2_005
	Sun JDK (Solaris Production Release) 1.1.6, 1.1.7B, 1.1.8_10, 1.2.1;
	Sun JDK (Solaris Reference Release) 1.1.6_007, 1.1.7B_005, 1.1.8_002, 1.2.1_003, 1.2.2_004;
	Sun JDK (Windows Production Release) 1.1.6_007, 1.1.7B_005, 1.1.8_002, 1.2.1_003, 1.2.2_004
		A security vulnerability exists due to untrusted Java code which could allow a malicious applet to be used to compromise the security of a host system.
		Note: To the best of Sun's knowledge, Netscape Navigator and Microsoft Internet Explorer are not exposed to this vulnerability.
			Update available at:
			Windows Production and Solaris Reference Releases:
			http://java.sun.com/products/jdk/
			Solaris Production Releases:
			http://www.sun.com/software/solaris/java/
			Linux Production Release:
			http://java.sun.com/products/jdk/1.2/download-linux.html
				Sun JDK/JRE Disallowed Class Loading	Medium	Bug discussed in newsgroups and websites.

[39] Securiteam, December 13, 2000.

[40] Bugtraq, December 8, 2000.

[41] Sun Microsystems, Inc. Security Bulletin, #00199, November 29, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Trlinux[42] Unix	Postaci Webmail 1.1.3	A vulnerability exists in the default configuration which may allow a remote malicious user to gain access to sensitive information about the operating system.	No workaround or patch available at time of publishing.	Postaci Webmail Password Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
University of Washington[43] Unix	pico 3.7-4.3	A vulnerability exists when the text editor abnormally exits which could let a malicious user symbolically link the file to one of owner/group write access of the user. This would result in the contents of the pico session being written to the symbolically linked file.	No workaround or patch available at time of publishing.	University of Washington Pico File Overwrite	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
VPNet Technologies[44]	VSU 100, 2000, 5000, 7500	Multiple vulnerabilities exist: Source routing flaw allows unauthenticated connections to a target host on a protected VPN; sensitive information is transferred in clear text; and a flaw in the NOS bridging code causes VSU to pass spoofed private address packets from its public interface to the private network.	No workaround or patch available at time of publishing.	VSU Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
VPNet Technologies[45]	VPNos 3.0	A vulnerability exists in the source routing of sessions which could allow a remote malicious user unauthorized access and the ability to potentially exploit hosts within the private network.	Upgrades available at: http://www.vpnet.com/slh97/Bulletins/securitynote.htm	VPNet VSU Source Routed Session	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[42] Bugtraq, November 30, 2000.
[43] Securiteam, December 14, 2000.
[44] Fate Research Labs, December 5, 2000.
[45] F8 labs Advisory, 20001205, December 6, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
WatchGuard Technologies, Inc.[46]	SOHO Firewall 1.6, 2.1.3	Multiple vulnerabilities exist: Weak Authentication; GET Request Buffer Overflow; Fragmented IP packet attack; and Password Reset using POST Operation, which could allow a remote malicious user to gain access to the administrative functions of the firewall without authenticating, crash the configuration server, or cause the device to stop accepting network traffic.	Upgrade available at: http://bisd.watchguard.com/SOHO/Downloads/swupdates.asp	Multiple SOHO Firewall Vulnerabilities	Low/ **High** **(High if DDoS best practices not in place).**	Bug discussed in newsgroups and websites. Exploit has been published.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between December 15, and December 1, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 39 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
December 15, 2000	Ao20pr_p.zip	Recovers lost passwords for Microsoft Word, Excel, Access, PowerPoint 97, Project, Money, Outlook, Backup, Schedule+, Mail, IE 3, 4, and 5, Visio 4 and 5, and others.

[46] Securiteam, December 15, 2000.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
December 15, 2000	**Rdc-lprng.c**	**LPRng v3.6.24 and below remote root exploit for Linux/x86 which exploits the syslog() format string vulnerability.**
December 15, 2000	Stunnel-3.9.tar.gz	Stunnel is a program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer) available on both Unix and Windows.
December 15, 2000	Xsold.C	Script which exploits the Linux Xsoldier local root buffer overflow vulnerability.
December 14, 2000	Helot.C	Script which exploits the BitchX Multiple Vulnerabilities.
December 14, 2000	Killntoe.C	Nettoe v1.0.5 Denial of Service attack.
December 14, 2000	**Sa_09.txt**	**Exploit URL's for the EZshopper v2.0 and v3.0 vulnerability.**
December 13, 2000	Ntomax20.zip	A scriptable server stress testing tool. This tool takes a text file as input and runs a server through a series of tests based on the input. The purpose of this tool is to find buffer overflows and DoS points in a server.
December 12, 2000	Angst-0.2b.Tar.Gz	An active packet sniffer, based on libpcap and libnet, which dumps into a file the payload of all the TCP packets received on the specified ports.
December 12, 2000	Dps-001.tgz	Distributed Port Scanner that scans multiple systems from different classes of networks. The user runs a central server that tells each client which port to scan next.
December 12, 2000	Dtors.txt	This paper presents a concise explanation of a technique to gain control of a C program's flow of execution given that it has been compiled with gcc. This exploit technique has several advantages over changing the stack pointer, including ease of determining the exact position where we want to write and point to our shellcode, and it is simpler than a GOTpatch.
December 11, 2000	Apcupsdos.C	Script which exploits the Apcupsd v3.7.2 local Denial of Service vulnerability.
December 11, 2000	**Mon_pine.sh**	**Script which exploits the Pine v4.30 and below outgoing mail vulnerability.**
December 11, 2000	Oopz.C	Script which exploits theMultiple Oops Proxy Server Buffer Overflow vulnerability.
December 11, 2000	Pkcoops-ex.c	Script which exploits theMultiple Oops Proxy Server Buffer Overflow vulnerability.
December 11, 2000	Saint-3.1.1.tar.gz	An updated version of SATAN.
December 11, 2000	**Shop.pl.txt**	**Exploit URL's for the Hassan Consulting's Shopping Cart Version 1.x (cgi-bin/shop.pl) vulnerabilities.**
December 8, 2000	Phonebook.C	Microsoft Phonebook Server Remote Exploit.
December 8, 2000	Wap-nmap-1.0.1.tar.gz	Wap-nmap enables a nmap scan from a WAP-enabled device and sends the results back to the device.
December 7, 2000	Bf-code.c	Denial of Service exploit for the Bftpd 1.0.12 remote buffer overflow vulnerability.
December 5, 2000	Hp-pppd.c	HP/UX v11.0 /usr/bin/pppd local root buffer overflow exploit.
December 5, 2000	Phpxpl.C	PHP 3.0.16/4.0.2 remote root format string overflow exploit for Linux/x86.
December 5, 2000	Wingate.C	Denial of Service exploit for Wingate 4.01.
December 5, 2000	Xlockfmt.C	Xlock local format string exploit for Linux/x86.
December 5, 2000	Ypbind.tgz	Linux/x86 remote root exploit for ypbind (ypbind-mt).
December 2, 2000	A120100-1.txt	Proof of concept exploit for Microsoft's SQL server buffer overflow vulnerabilities.
December 2, 2000	A120100-2.txt	Proof of concept exploit for Microsoft SQL Server vulnerability.
December 2, 2000	Bsdi_sperl.c	BSDI 3.0 /usr/bin/suidperl local root exploit.
December 2, 2000	Libc-language.su.c	Glibc 2.1 + /bin/su local root exploit.
December 2, 2000	Lnapster_dos.c	Script which exploits the Linux Napster Client v0.9 through v1.4.4 remote Denial of Service vulnerabilities.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
December 2, 2000	Mogrify.C	Script which exploits the usr/X11R6/bin/mogrify local buffer overflow vulnerability.
December 2, 2000	Nsat-1.23.tgz	A fast, stable bulk security scanner designed to audit remote network services and check for versions, security problems, and gather information about the servers and the machine.
December 2, 2000	Sendip-1.3.tar.gz	A commandline tool to send arbitrary IP packets which has a large number of command line options to specify the content of every header of a TCP, UDP, ICMP, or raw IP packet.
December 2, 2000	Spoofaudit_0.1.3.tar.gz	A Perl tool which helps you determine what basic spoofing filters are present between two test points on two networks, and what anti-spoofing filters are missing.
December 2, 2000	Sqladv2-poc.c	This code creates a file called 'SQL2KOverflow.txt' in the root of the C: drive.
December 2, 2000	Tessa.C	Remote denial of service exploit for Microsoft Exchange 5.5 SP3 Internet Mail Service and Information Store vulnerability.
December 2, 2000	Xp-bitchx.c	Script which exploits the BitchX v1.0c16 vulnerability.
December 1, 2000	Sqladv2-pop.c	Script which exploits the Microsoft Extended Stored Procedure Parameter Parsing vulnerability.
December 1, 2000	Sqladv-pop.c	Script which exploits the Microsoft Extended Stored Procedure Parameter Parsing vulnerability.

Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

No scripts were submitted during the two-week period covered by this issue of CyberNotes.

Trends

DDoS/DoS:

The Cert Coordination Center recently issued an alert regarding Denial of Service vulnerabilities in TCP/IP stacks. For more information, please see CERT Advisory CA-2000-21, located at: http://www.cert.org/advisories/CA-2000-21.html.

The CERT Coordination Center has recently issued an alert regarding of two serious Denial of Service vulnerabilities in the Internet Software Consortium's (ISC) BIND software. For more information, please see CERT Advisory CA-2000-20, located at: http://www.cert.org/advisories/CA-2000-20.html.

Probes/Scans:

An increase in the number of NETBIOS Session (139/tcp) probes.

Intruders are using scripts and toolkits to automate attacks against the input validation problem in rpc.statd and the input validation problems in FTPD, the site exec vulnerability. For more information, see the CERT advisory located at: http://www.cert.org/incident_notes/IN-2000-10.html.

A number of sites have been compromised by exploiting a vulnerability in the IRIX telnet daemon. Intruders are actively exploiting a vulnerability in telnetd that is resulting in a remote root compromise of victim machines.

Other:

The NIPC has been tracking the W32/ProLin@MM Internet worm (Shockwave) and currently assesses that it represents a medium threat in the United States. For more information, please see NIPC Assessment 00-061 located at: http://www.nipc.gov/warnings/assessments/2000/00-061.htm

A new Internet worm, I-Worm.XTC, is using a technique of searching cached pages for e-mail addresses. Many antiviral warning systems will not detect its presence until specific detection signatures are added for it.

A recent NIPC Assessment states that a regional entity in the electric power industry has recently experienced computer intrusions through the Anonymous FTP (File Transfer Protocol) Login exploitation. For more information, please see NIPC Assessment 00-062 located at: http://www.nipc.gov/warnings/assessments/2000/00-062.htm.

A continuing increase in reports of computers infected with the QAZ Trojan.

Several instances of remote self-updating viruses have been reported. In addition, the most recent virus incorporates strong cryptography to avoid detection.

NIPC has issued an assessment on the W32 Navidad@M Worm. For more information, please see NIPC Assessment 00-059 located at: http://www.nipc.gov/warnings/assessments/2000/00-059.htm.

Viruses

A list of viruses infecting two or more sites as reported to various anti-virus vendors has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. These types of malicious code will now be included in the table where appropriate. Following this table are write-ups of new viruses and updated versions discovered in the last two weeks. WARNING: at times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **213** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **598** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Ranking	Common Name	Type of Code	Trends	Date
1	VBS/LoveLetter	Script	Stable	March 2000
2	PE_MTX.A	File Infector, Trojan	Slight increase	September 2000
3	VBS/Kakworm	Script	Slight decrease	December 1999
4	W32/SKA	File	Increase	March 1999
5	VBS/Stages	Script	Slight decrease	June 2000
6	W97M/Marker	Macro	Increase	August 1998
7	W97M/Ethan.A	Macro	Decrease	February 1999
8	FunLove	File	Slight increase	November 1999
9	W32/PrettyPark	File	Return to table	June 1999
10	W95/CIH	File	Return to table	April 1999

ELF_X21 (Alias: X2) (Elf Executor Virus): This virus infects Unix files by overwriting them with its code and renaming the original host file (the uninfected file) with an extension of .X21.

O97M_TRISTATE (Aliases: TRISTATE, O97M_TRIPLICATE, TRIPLICATE, X97M_TRISTATE, P97M_TRISTATE, W97M_TRISTATE) (Office 97 Macro Virus): This macro virus cross-infects Microsoft Word 97, Microsoft Excel 97, and Microsoft PowerPoint 97 applications. Upon activation in Excel the virus searches for BOOK1.XLS in the Excel Startup directory. If not found, the virus creates an infected workbook in the same directory and disables Excel's macro virus protection. The virus resides in the "ThisWorkbook" stream of an infected excel spreadsheet/workbook. When activated in Word, the virus will check for its codes in the "ThisDocument" Stream of the Global Template (NORMAL.DOT). If not found, the virus infects the global template and disables Word's macro virus protection. When the virus activates in PowerPoint, the virus searches for the "Triplicate" module in the "BLANK PRESENTATION.POT" PowerPoint Template. If not found, the virus disables PowerPoint's macro virus protection. The virus then adds a viral module called "Triplicate" into "BLANK PRESENTATION.POT" and a basic AutoShape object that covers the entire slide. The viral module is linked to the AutoShape object.

PE_KRIZ.4050 (Aliases: KRIZ.4050, W32/Kriz.4050, W32. Kriz.4050, W32.Kriz.4050.kernel, W95.Kriz) (File Infector Virus): This polymorphic Windows executable virus infects EXE files. It may also destroy some type of PC's Flash BIOS (similar to PE_CIH) and the infected computer's CMOS information.

PE_SPACES.1445 (Aliases: W95/SPACES.1445, W95/BUSM.1445, SPACES.1445) (File Infector Virus): This destructive Windows virus destroys the Master Boot Record (MBR) of the system hard disk if the current system date is June 1. Due to this, the virus also causes boot-up failure. It is memory resident and is capable of infecting both Windows 9x and Windows NT 4.0 systems.

VBS/Forgotten-A (Visual Basic Script Worm): This is a VBS worm that uses Microsoft Outlook to spread. It arrives in an HTML e-mail message with no attachments. The subject of the message is "RE: Financing ." The message body is set by the embedded VBScript. If the Internet security setting is configured to disallow the running of unsafe ActiveX controls, the message text will be "You need ActiveX enabled if you want to see this e-mail. Please open this message again and click accept ActiveX Microsoft Outlook ." If unsafe ActiveX controls is enabled, the message will be "YOU WILL NOT FORGET THIS MOMENT, NEVER!" The worm drops a VBScript file VB1.COM.VBS into the Windows system directory and runs it. This script attempts to create an e-mail message with the worm VBS code embedded and sends it to all contacts in the user's Outlook address book. The dropped VBS file also searches mapped drives, shared drives, and all other active drives for files with the extension VBS or VBE and overwrites them with a copy of itself. If the PIRCH or mIRC IRC clients are installed, the worm also drops scripts that attempt to send the dropped VBScript file to other mIRC users.

VBS/Kakworm-E (Visual Basic Script Worm): This is a variant of the VBS/Kakworm worm. The worm only affects users using Microsoft Outlook Express 5 as the e-mail client. If the user opens or previews an infected e-mail message, the worm drops the file EXEC.HTA into the Windows startup folder so that it runs automatically when Windows is started. The EXEC.HTA file creates a hidden file called C:\WINDOWS\EXC.HTM and changes the Microsoft Outlook Express Registry settings so that the EXC.HTM is automatically included in every outgoing message as a signature file. If a file called G6D9.fld exists in the system directory, the worm also attempts to change the Windows Registry so that the Windows Notepad application is executed in place of any EXE program file.

Microsoft has released a patch to deal with this security problem which we strongly recommend users install. For further information and to download the patch please view Microsoft Security Bulletin (MS99-032).

VBS/LoveLet-CA (Visual Basic Script Worm): This is a variant of the VBS/LoveLet-CA Visual Basic Script worm. The main difference in this variant is that on December 25th it displays a message box including the text:

EVEN TRENT KNOWS ITS TRUE=>STARFUCKERS INC. Att. REJOH (REDRUM)

where 'REJOH' can be any random 5 letters. The worm forwards itself as an e-mail attachment with the subject line: US PRESIDENT AND FBI SECRETS =PLEASE VISIT => (http://WWW.2600.COM)<= or a random 6 letter string. The message body will either be:

VERY JOKE..! SEE PRESIDENT AND FBI TOP SECRET PICTURE..

or a random 10 letter string. Running the attached file infects your computer.

VBS/Season (Visual Basic Script Worm): This is a Visual Basic Script worm. When an infected VBS file is launched, it displays a message box with the title "Important Message: Bill Gates" and the text "This is a very important message from Bill Gates. New Virus Will be out this season, look out for it!! ." Pressing 'OK' brings up a second message box with the title "Important Message" and the text "There will be a text file on your desktop. Please Read Carefully ." The virus creates a file called IMPORTANTMESSAGE.TXT on the desktop. The virus also copies itself to the following files:

C:\Windows\important.txt.vbs
C:\important.txt.vbs
C:\Windows\system\important.txt.vbs
C:\MyDocuments\important.txt.vbs

The .VBS extension is often hidden by Windows Explorer. If mIRC (Internet Relay Chat) is installed, the virus will also overwrite the SCRIPT.INI file so that a copy of the virus is sent to other users who join the same chat channels. The virus creates a file called C:\WINDOWS\Start Menu\Programs\StartUp\ SpreadByADrive.txt.vbs that attempts to copy the virus to a floppy disk on Windows Startup. Finally, the virus overwrites AUTOEXEC.BAT with instructions to display the message "Important Message!! Message From Bill Gates New viruses is out this season!!! Look Out!!!" and then attempts to delete all .TXT, .MP3, .BMP, .JPG, .GIF, .ZIP, .EXE and .WAV files from the C:\MyDocument directory upon boot up.

W32/Hybris-B (Win32 Worm): This worm has been reported in the wild. It is capable of updating its functionality over the Internet and consists of a base part and a collection of upgradeable components. The components are stored within the worm body encrypted with 128-bit strong cryptography. When run, the worm infects WSOCK32.DLL. Whenever an e-mail is sent, the worm attempts to send a copy of itself in a separate message to the same recipient. The text of the e-mail message is determined by one of the installed components, and can be changed by the upgrading mechanism. Versions of the worm check the language settings of the computer it has infected, and select a message accordingly from: English, French, Portuguese, and Spanish. The methods for upgrading the worm can also be changed since they are upgradable components. One of the upgrading techniques attempts to download the encrypted components from a website. This website has been disabled. However, this component could be upgraded to have a different web address. The other method involves posting its current plug-ins to the Usenet newsgroup alt.comp.virus, and upgrading them from other posts by other infections of the worm. These are also in the encrypted form, and have a header with a four-character identifier and a four-character version number, in order for the worm to know which plug-ins to install. Another component of the worm searches the PC for .ZIP and .RAR archive files. When it find one, it searches inside it for a .EXE file, which it renames to .EX$, and then adds a copy of itself to the archive using the original filename. There is a payload component, which on the 24th of September of any year, or at 1 minute to the hour at any day in the year 2001, displays a large animated spiral in the middle of the screen.

W32/Hybris-C (Win32 Worm): There have been several reports of the worm in the wild. It is capable of updating its functionality over the Internet and consists of a base part and a collection of upgradeable components. The components are stored within the worm body encrypted with 128-bit strong cryptography. When run, the worm infects WSOCK32.DLL. Whenever an e-mail is sent, the worm attempts to send a copy of itself in a separate message to the same recipient. The text of the e-mail message is determined by one of the installed components, and can be changed by the upgrading mechanism. Versions of the worm check the language settings of the computer it has infected, and select a message accordingly from: English, French, Portuguese, and Spanish. The methods for upgrading the worm can also be changed since they are also upgradable components. There is a payload component, which on the 24th of September of any year, or at 1 minute to the hour at any day in the year 2001, displays a large animated spiral in the middle of the screen. There is also a component that applies a simple polymorphic encryption to the worm before it gets sent by e-mail. By upgrading this component, the author is able to completely change the appearance of the worm in unpredictable ways in an attempt to defeat anti-virus products detecting it.

W32/Navidad (Aliases: W32/Watchit, w32/navidad@m) (Windows 32 Executable File Virus): There have been several reports of this virus in the wild. It is an e-mail worm that arrives in an e-mail message with an attachment called NAVIDAD.EXE. If the attached program is launched, it displays a dialog box containing the text "UI.” The virus then attempts to read new e-mail messages and to send itself to the senders' addresses. The virus also copies itself into the Windows system directory with the filename WINSVRC.VXD and changes the registry so that it runs on Windows startup and before any file is run. Next the virus installs itself into the system tray. If the user clicks on the icon, it displays a dialog box with the text "Nunca presionar este boton.” If the user clicks the button, the worm displays a dialog box with the title "Feliz Navidad" and the text "Lamentablemente cayo en la tentacion y perdio su computadora.”

W32/Xtc (Aliases: I-Worm.XTC, W32/XTC@MM) (Win32 Worm): This is an e-mail worm which spreads across network shares. If received via e-mail, the worm arrives in the form of an e-mail attachment (usually called SERVICES.EXE) to a message claiming to be from the e-mail address support@avx.com. The message's subject line is: “AVX update notification .” When the worm is run, it will install itself and then attempt to connect to an Undernet IRC (Internet Relay Chat) server. It announces its presence on a channel on the IRC server and can then be controlled and updated by a remote user or other instances of the worm itself. The worm includes facilities to upload, download and run files on the infected machine and launch distributed Denial of Service attacks.

W97M_CHINGDA.TRJ (Alias: CHINGDA.TRJ) (Word 97 Macro Virus): This virus is activated when opening and closing documents. It alters the contents of the active document and loses its original form.

W97M/Ozwer.A (Word 97 Macro Virus): This is a virus which infects Microsoft Word 97 documents and the NORMAL.DOT global template the application uses. When an infected document is opened, the virus checks if the NORMAL.DOT global template is infected. If it isn't, then it is infected and saved. Once the template has been infected it will proceed to infect the documents which use it as a basis. W97M/Ozwer.A also disables the options that allow users to handle macros in Microsoft Word documents.

W97M/Admin (Word 97 Macro Virus): This is a virus which infects Microsoft Word 97 documents and the NORMAL.DOT global template the application uses. When an infected document is opened, the virus checks if the NORMAL.DOT global template is infected. If it isn't, then it is infected and saved. Once the template has been infected it will proceed to infect the documents which use it as a basis. W97M/Admin creates a file called SYSTEM.DLL in the Windows directory (generally in C:\WINDOWS).

WM97/Ded-J (Word 97 Macro Virus): This is a variant of WM97/Ded-B. Unlike other family members this variant has no polymorphic capabilities or malicious payload.

WM97/Marker-FX (Word 97 Macro Virus): This is a variant of the WM97/Marker Word macro virus. It has no active malicious payload and only replicates.

WM97/Metys-E (Word 97 Macro Virus): This is a variant of WM97/Metys-D. On 1 September the virus displays a message box:

> "Happy Birthday Jess! To celebrate, we're going to see how lucky
> you are <Username>. Click the OK button below to roll a number.
> If your number matches that of the dealer, you win!"

WM97/Shore-D (Word 97 Macro Virus): This virus changes local customisations and format style, and protects the Visual Basic code with the password "cool13 ." In addition, three seconds after loading or closing the document it displays a message for a short time in the Microsoft Word title bar: "Offshore Engineering - Peace at the sea... ." It also creates a template file "Offee*.dot" in the clipart directory.

WM97/Thus-BF (Word 97 Macro Virus): This is a Word macro virus. When documents infected by this variant of the WM97/Thus family are opened, VB runtime errors will be displayed. However, the virus still manages to spread to other documents.

XM97/Fusion-A (Excel 97 Macro Virus): This is an Excel macro virus that attempts to delete the files HJB.XLS, 874.XLS and KHM.XLS if found in the XLSTART directory. These files are dropped by other Excel macro viruses. XM97/Fusion-A then creates its own file called FUSION.XLS in the XLSTART directory.

XM97/Laroux-EH (Excel 97 Macro Virus): This is an Excel spreadsheet macro virus, created by the merging of a user macro and the XM97/Laroux-BK virus.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in CyberNotes. This table includes Trojans discussed in the last six months and will be updated on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	Issue discussed
Asylum + Mini	v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1	CyberNotes-2000-10, CyberNotes 2000-12
AttackFTP		CyberNotes-2000-10
Backdoor/Doly.17		CyberNotes-2000-16

Trojan	Version	Issue discussed
BackDoor-GZ		CyberNotes-2000-18
BackDoor-HC		CyberNotes-2000-18
Backdoor-HD		CyberNotes-2000-18
BCK/Sub7.Apocalypse		CyberNotes-2000-23
BF Evolution	v5.3.12	CyberNotes-2000-10
BioNet	v0.84 - 0.92 +2.2.1	CyberNotes-2000-09, CyberNotes 2000-12
Bla	1.0-5.02, v1.0-5.03	CyberNotes 2000-09
Bobo	v1.0 - 2.0	CyberNotes-2000-09
Donald Dick 2		CyberNotes-2000-15
Drat	v1.0 - 3.0b	CyberNotes-2000-09
Erap Estrada		CyberNotes-2000-18
GIP		CyberNotes-2000-11
Golden Retreiver	v1.1b	CyberNotes-2000-10
Hooker-E		CyberNotes-2000-19
ICQ PWS		CyberNotes-2000-11
InCommand	1.0-1.4, 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes-2000-09
iniKiller	v1.2 - 3.2, 3.2 Pro	CyberNotes-2000-09, CyberNotes-2000-10
JS_SEEKER.B		CyberNotes-2000-22
Kaos	v1.1 - 1.3	CyberNotes-2000-10
Khe Sanh	v2.0	CyberNotes-2000-10
Magic Horse		CyberNotes-2000-10
Matrix	1.4-2.0, 1.0-2.0	CyberNotes-2000-09
Mosaic	v2.00	CyberNotes-2000-16
Multijoke.B		CyberNotes-2000-15
Naebi	v2.12 - 2.39, v2.40	CyberNotes-2000-09, CyberNotes 2000-12
Netbus.153		CyberNotes 2000-16
Netbus.170		CyberNotes 2000-16
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
Netsphere.Final		CyberNotes-2000-15
NoDesk		CyberNotes-2000-14
Omega		CyberNotes 2000-12
Palm/Liberty-A		CyberNotes-2000-18
PALM_VAPOR.A		CyberNotes-2000-19
PE_MTX.A		CyberNotes-2000-18
Phaze Zero	v1.0b + 1.1	CyberNotes-2000-09
Prayer	v1.2 - 1.5	CyberNotes-2000-09
Prosiak	beta - 0.65 – 0.70 b5	CyberNotes-2000-09, CyberNotes 2000-12
Qaz.A	W32.HLLW.Qaz.A	CyberNotes-2000-20, CyberNotes-2000-16
QDel121		CyberNotes-2000-23
Revenger	1.0-1.5	CyberNotes 2000-12

Trojan	Version	Issue discussed
Serbian Badman		CyberNotes 2000-12
ShitHeap		CyberNotes-2000-09
Snid	1-2	CyberNotes 2000-12
SubSeven	DEFCON8 2.1 Backdoor	CyberNotes-2000-21
Troj/Simpsons		CyberNotes-2000-13
TROJ_AOL_PS.A		**Current Issue**
TROJ_BATMAN		CyberNotes-2000-20
TROJ_BLEBLA.A		CyberNotes-2000-24
TROJ_BLEBLA.B		CyberNotes-2000-24
TROJ_BLOODLUST		CyberNotes-2000-21
TROJ_BUTANO.KILL		CyberNotes-2000-19
Troj_Dilber		CyberNotes-2000-14
TROJ_ENERGY.A		CyberNotes-2000-24
TROJ_FELIZ		CyberNotes-2000-22
TROJ_ICECUBES.A		CyberNotes-2000-24
TROJ_IGMNUKE		CyberNotes-2000-20
TROJ_IRCKILL		**Current Issue**
TROJ_KILLME		CyberNotes-2000-20
TROJ_MSINIT.A		CyberNotes-2000-21
TROJ_MUSIC.A		CyberNotes-2000-24
TROJ_MUSIC.B		**Current Issue**
TROJ_MUSIC.C		**Current Issue**
TROJ_MUSIC.D		**Current Issue**
TROJ_MYPICS.F		CyberNotes-2000-23
TROJ_NAVIDAD.A		CyberNotes-2000-23
TROJ_NAVIDAD.E		CyberNotes-2000-24
TROJ_ORION		CyberNotes-2000-24
TROJ_PERSONAL_ID		CyberNotes 2000-16
TROJ_POKEY.A		CyberNotes 2000-16
TROJ_ROCKET		CyberNotes-2000-22
TROJ_SCOOTER		CyberNotes-2000-19
TROJ_SHOCKWAVE.A		CyberNotes-2000-24
TROJ_SONIC		CyberNotes-2000-22
TROJ_SPAWNMAIL.A		CyberNotes-2000-18
TROJ_SUB7.214DC8		CyberNotes-2000-21
TROJ_SUB7.382883		CyberNotes-2000-21
TROJ_USSRHYMN.A		CyberNotes-2000-24
TROJ_VBSWG		CyberNotes-2000-16
TROJ_XTC.A		**Current Issue**
Trojan/Anything		CyberNotes-2000-23
Trojan/ICQ		CyberNotes-2000-20
Trojan/Parkinson		CyberNotes-2000-21
Trojan/PSW.StealthD		CyberNotes-2000-19
Trojan/Ring0.B		CyberNotes-2000-24
Trojan/Twinshoe		CyberNotes-2000-24
Trojan/Varo31		CyberNotes-2000-19
Trojan/Win32		CyberNotes-2000-21
VBS_MAILPEEP		CyberNotes-2000-22

Trojan	Version	Issue discussed
W32.Nuker.C		CyberNotes-2000-14
Win.Unabomber		CyberNotes-2000-14
WinCrash	Beta	CyberNotes-2000-12
Winkiller		CyberNotes 2000-12

TROJ_AOL_PS.A (Alias: AOL Software): This Trojan is in NE (Non Executable) format and is written in Visual Basic. It cannot run properly if the VBRUN300.DLL file is not found. It is an AOL Password Stealer which records keystrokes immediately after AOL is triggered. This Trojan is a security threat, since it can obtain a user's AOL password.

TROJ_IRCKILL (Aliases: Flooder.IRCKill, IRCKILL): This Trojan is a collection of IRC tools used to disconnect users logged onto the IRC network. It consolidates the functions of flooding, use of multiple-collide bots or sumo bots, and flash, which is a type of flooding intended for the Unix environment.

TROJ_MUSIC.B (Aliases: MUSIC WORM, MUSIC.B): This Trojan, upon execution, displays a graphic and plays a tune. It also modifies the registry and drops files so that the Trojan is executed at every Windows start up. It uses the Microsoft Messaging API to propagate and sends itself as an e-mail attachment to all lists in the Windows Address book of the infected user. It is a variant of TROJ_MUSIC.A.

TROJ_MUSIC.C: This network-enabled Trojan is disguised as a simple program that displays graphics and plays a tune. Upon execution, it modifies the Windows registry and drops files to propagate via e-mail. The Trojan has the capability to download potentially malicious upgrades from the Internet and is a variant of TROJ_MUSIC.A.

TROJ_MUSIC.D (Aliases: MUSIC.D, W95/Music@M, I-Worm.Music.D): This network-enabled Trojan is disguised as a simple program that displays graphics and plays a tune. Upon execution, it modifies the Windows registry and drops files to propagate via e-mail. The Trojan has the capability to download potentially malicious upgrades from the Internet.

TROJ_XTC.A (Aliases: I-Worm.XTC, XTC.A): This Trojan comes as an e-mail attachment called SERVICES.EXE. It is disguised as an AVX 2000 (AntiVirus eXpert 2000) update and carries the AVX icon. Upon execution, it uses e-mail addresses found in HTML and HTM files as recipients of the spam e-mail attachment SERVICES.EXE.